Does your employer have to tell if they're spying on you through your work computer?

October 10 2023, by Jacqueline Meredith and Peter Holland

Credit: AI-generated image (disclaimer)

The COVID pandemic stimulated an irreversible shift in where, when and how we work. This 21st-century model of working—dubbed the "new normal"—is characterized by increased flexibility and productivity gains.

Yet this reshaping of work, underpinned by technology, has also eroded our work-life boundaries—and persisting 20th-century attitudes are preventing us from successfully managing the new normal.

We find ourselves struggling with "productivity paranoia": a term used to describe managers' concerns that remote and hybrid workers aren't doing enough when not under supervision.

As a result, we're seeing a surge in the use of electronic monitoring and surveillance devices in the workplace. These devices allow managers to "watch over" employees in their absence. This practice raises serious legal and ethical concerns.

Big bossware is here

In a survey of 20,000 people across 11 countries, Microsoft reported 85% of managers struggled to trust their remote-working employees. In Australia, this figure was 90%.

In 2021, American research and consulting firm Gartner estimated the number of large firms tracking, monitoring and surveilling their workers had doubled to 60% since the start of the pandemic.

Electronic monitoring and surveillance technology can capture screenshots of an employee's computer, record their keystrokes and mouse movements, and even activate their webcam or microphones.

On one hand, these "bossware" tools can be used to capture employee and production statistics, providing businesses with useful evidence-based analytics.

The other side is much darker. These devices are indiscriminate. If you're working from home they can pick up audio and visual images of

your private life.

Managers can be sent notifications when data "indicate" an employee is taking breaks or getting distracted.

Some aspects of electronic monitoring and surveillance are legitimate. For instance, it may be necessary to safeguard an organization's data access and transfers.

But where are the boundaries? Is your organization legally obliged to tell you about electronic intrusions? Alternatively, what can you do if you find out you're being watched without being informed?

The legal framework

A complex array of regulation governs workplace privacy and surveillance in Australia. Proposed reforms to the Privacy Act 1988 are set to strengthen privacy protections for private-sector employees.

However, this legislation doesn't specifically cover workplace surveillance. Instead, a patchwork of laws in each state and territory regulate this matter.

Specific legislation regulates the surveillance of workers in New South Wales and the Australian Capital Territory. Importantly, surveillance must not be undertaken unless the employer has provided at least 14 days' notice. This notice must include specific details about the surveillance that will be carried out. Employers must also develop and adhere to a surveillance policy.

In both states, employers can only record visual images of an employee while they're "at work". This is broadly defined to capture any place where work is carried out.

Covert surveillance is prohibited unless the employer has obtained a court order. In this case it's restricted to situations where the employee is suspected of unlawful activity.

Even then, a covert surveillance order would not be granted where this unduly intrudes on the employee's privacy. Covert surveillance for the purpose of monitoring work performance is expressly prohibited.

Other states and territories don't have specific electronic workplace surveillance laws. Employers must instead comply with more general surveillance legislation.

Broadly speaking, employees must give consent, express or implied, to any surveillance. In practice, such consent is usually obtained through the implementation of a workplace surveillance policy, which employees must agree to when they accept the job. So if you've signed a contract without reading the fine print, you may have agreed to being surveilled via electronic monitoring tools.

Currently, Queensland and Tasmania provide the most limited protection for employees. Their surveillance legislation is limited to the regulation of listening devices.

Enterprise agreements, employment contracts and workplace policies may also limit or prohibit the use of surveillance devices. In practice, however, most employees will lack the bargaining power to negotiate the inclusion of any such terms in their employment contract.

The law is failing to keep up

In 2022, a parliamentary select committee reporting on the future of work in NSW observed the current regulatory framework is failing to keep pace with rapid advancements in electronic monitoring and

surveillance.

The report criticized legislation that simply allows an employer to notify workers surveillance will be carried out, with no mechanism for this to be negotiated or challenged. The situation is slightly better in the ACT, where employers must consult with workers in good faith about any proposed surveillance activities.

Workers who suspect their employer is spying on them should review their workplace surveillance policies. They may need to reflect carefully on how they use their work computer.

Where an enterprise agreement applies, the Fair Work Commission can arbitrate surveillance disputes. A worker who is dismissed following intrusive surveillance may be able to challenge the dismissal on the basis of it being unfair.

Workers who haven't been informed of their employer's surveillance practices can also lodge a complaint with the relevant authority or regulator, who may have powers to investigate and prosecute offenses.

To thrive in our "new normal" work landscape, we'll need to address the gap between the existing legal protections and the capabilities (and potential harms) of electronic monitoring and surveillance. For now, it remains a significant legal and ethical challenge.

Provided by The Conversation

Citation: Does your employer have to tell if they're spying on you through your work computer?